Defense Manpower Data Center

DID YOU KNOW? JPAS NEWSLETTER

SERVING THOSE WHO SERVE OUR COUNTRY

2ND QUARTER CY2015

ISSUE: 2015-2

THIS ISSUE FEATURES

DMDC CONTACT CENTER CHANGES

Starting 1 June 2015, the Defense Manpower Data Center (DMDC) Personnel Security/Assurance (PSA) Contact Center will be modifying its hours to be open from 8 AM Eastern Time (ET) to 8 PM ET, Monday through Friday, excluding Federal holidays. This is a change from the previous hours of 6 AM ET to 8 PM ET. There will be little impact to customers as call volume from 6 - 8 AM ET were very low.

For further information and any other updates regarding the DMDC Contact Center, please see the JPAS Contact Customer Service webpage.

Find us on Facebook

Join us and start connecting with DMDC at:
http://www.facebook.com/go2dmdc

JPAS USER ACCOUNT AUDIT TRENDS

While implementing the guidance from the Department of Defense (DoD) Privacy Program, DoD 5200.11-R (May 4, 2007), regulation C1.2 through C1.2.2 (Standard of Accuracy) and DoD personnel security polices, DMDC generated monthly user audit reports and as a result, have identified several trends that pose potential risk to the DoD Personnel Security Program. The main three trends are Incorrect Legal Name, Test or Fake SSNs, and Viewing One's Own Record.

Incorrect Legal Name - The DoD Privacy Act Regulation requires the use of a legal name in the Joint Personnel Adjudication System (JPAS). In reviewing the data, it appears that many names in JPAS are nicknames and not the legal name as written on a subject's SSN and/or passport (e.g., Bob vs Robert, Mary vs Maryann). Please review all JPAS person information to ensure the name fields only contain the subjects' LEGAL NAME. If it is not accurate, please update the name per the JPAS Data Correction Checklist and use proper syntax for the Joint Verification System (JVS) Data Migration (click link for Proper Syntax). This could mean that the subject needs to go to their personnel center, Person Data Repository (PDR), or security office. Non-compliance could result in a user's account being locked until their legal name is corrected.

Inserting, Using or Testing Fake Social Security Numbers - As part of the JVS Data Migration, DMDC audited users who were inputting or using test/dummy SSNs in order to clean up the database prior to migration. DoD Regulations and the DMDC JPAS Account Management policies prohibit users from entering or using false or inaccurate information including entering test or "dummy" personal information into the DoD personnel security system of records. JPAS is a fully audited database that reflects each time a user selects, adds, modifies, or deletes anything in JPAS.

Look Up or View Your Own Record - As part of the JPAS User Monthly Audit, JPAS systematically audits the database for various misuses, to include users who query and/or look up their own record by viewing their Person Summary screen in JCAVS or selected themselves in JAMS. The DMDC JPAS Account Management Policy states that all users consent to the terms of use of the DoD System of Records and agree to comply with the Privacy Act of 1974, applicable DoD regulations, other applicable laws, and JPAS policies. The Account Management policy prohibits users from querying and/or looking up their own records in the DoD Personnel Security System of Records. This also constitutes a DoD Privacy violation and a misuse of JPAS.

GENERAL FAQ DOCUMENT UPDATES

The JPAS General Frequently Asked Question (FAQ) document was updated on 30 April 2015 to streamline existing content and add a section concerned with the administrative review (JPAS security incident) process. All JPAS users should be aware of the administrative review process, especially those users involved in a potential or alleged system misuse. It is critical to know that if a user is placed under an administrative review, their accounts will be locked and inaccessible for the duration of the review. They will be provided direct correspondence regarding the incident.

In order for users to avoid an administrative review it is important that each user is familiar with the terms and conditions set forth in the JPAS disclosure screen that every user agrees to before logging onto the system. Additional specific misuses that users must avoid can be found both in the General FAQ and the JPAS Account Management Policy. The list of misuses contained in these documents are not comprehensive, but are the most common scenarios that have been encountered.

The length of time that an administrative review may take varies dependent upon several factors and has no defined timeframe.

UPCOMING DQIS

Military Separations— JPAS has worked with DoD Service Personnel Centers in order to update separation dates on subject categories that have previously been out-processed from the Military.

DoD Identifiers posted to Industry records—in support of SIPRnet token issuance, the JPAS team provided Industry subjects to the DoD PDR. One result of this initiative is that subjects with Industry only categories will not be able to have their FSOs update their personal data (name, DOB, etc) in JPAS. Subjects with an Electronic Data Interchange Personal Identifier (EDIPI) on their JPAS record will have to follow the procedures outlined in the JPAS Data Correction Checklist in order to identify what they need to do to update their data moving forward.

Data cleanup in support of JVS migration—several records will be automatically corrected to ensure they will work consistently in the new JVS database. This effort includes eliminating invalid characters in subject names (such as spaces, apostrophes and other special characters), and removal of invalid birth or death dates.

Inserting Closed Investigation Statuses or Dates—the JPAS team is working with the Office of Personnel Management (OPM) to ensure that all older investigations properly reflect closed statuses and their corresponding dates.

SUBJECTS REQUIRING PERIODIC REINVESTIGATIONS

In order to complete the requirements identified in the Director of National Intelligence (DNI) memorandum "Strategy to Reduce the Periodic Reinvestigation Backlog Using a Risk-Based Approach," DMDC is working with the Military Services, DoD Agencies, and DSS (for Industry) to ensure that all JPAS subjects who do not have supporting, in-scope investigations no longer have access. As a result SOs/FSOs might be contacted in order to initiate re-investigations on subjects with out-of-scope investigations. If re-investigations are not opened on these subjects, the subjects may be administratively debriefed from access and lose their favorable eligibility. Data will be provided to identified service and agency POCs directly starting the week of 1 June.

Please make any and all efforts possible to ensure subjects are reinvestigated along the proper timelines.

PKI UPDATES

On 19 June, JPAS is updating its local traffic managers with new hardware and firmware. This will ensure that users will have Transportation Layer Security (TLS) 1.2 compatibility. Previously, JPAS was only able to communicate up to TLS 1.1 which caused some issues with users that were still on older browser versions such as Internet Explorer 9 as the browser was not able to negotiate the proper protocol when attempting to login. The upcoming migration will assist users of all browser versions potentially have a more secure connection to JPAS with fewer potential logon issues.

Did You Know???

JPAS Account Management Policy

Please ensure all Security Officers and Facility Security Officers are aware of the JPAS Account Management Policies .

JPAS Reports…

Remember that you can use the "background and pickup later" option when generating reports. This can help ensure that reports are properly rendered when immediate delivery may not work. Remember they are only stored for 48 hours once completed.

Protecting PII…

Never send a person's SSN without encryption. All JPAS related customer email addresses have

encryption capability.

Also note that all JPAS information is protected by the Privacy Act of 1974 and requires appropriate protection at all times.

REMINDERS

ACTION REQUIRED! SECURITY MANAGEMENT OFFICE (SMO) CONTACT INFORMATION UPDATE:

SMO Points of Contacts need to ensure that their SMO Contact Information is current and in the correct format. Only the correct format will be accepted. Those with information in an incorrect format will not receive pertinent information such as messages concerning the JCAVS to JVS migration, Continuous Evaluation updates, etc. The following Email Address and Phone Number format are REQUIRED:

Email Address field should **ONLY** contain an email address with NO additional wording before or after the email address.

Correct Format: jane.doe@email.com
Incorrect Format: For visit requests, email jane.doe@email.com

Additional email addresses should be separated only by a semi-colon (;)
Example: jane.doe.civ@mail.com; jane.doe.ctr@mail.mil

Phone Number format: Country Code + Area Code + Phone Number.

ACCOUNT ACTIVITY REMINDER AND PKI REGISTRATION

An active JPAS account is one that has been logged into within the past 30 days. If you do not login with in 30 days, know that your account will be deleted in accordance with CYBERCOM TASKORD 13-0641.

Also note that if you are a new account applicant, that the 30 day timer starts from the point the account is created, and not from the first time that you logon to the account using your PKI credential. It can take time to get an identity verified and an associated PKI credential issued, so please try to plan accordingly and have your PKI on hand **before** submitting a Personnel Security System Access Request (PSSAR) form for a JPAS account.

KEY MANAGEMENT PERSONNEL (KMP)

The authoritative file for Industry Key Management Personnel (KMP) is the Defense Security Services' (DSS) Industrial Security Facilities Database (ISFD). If you are a KMP for your company, please ensure your information and status is properly updated in the ISFD as JPAS and ISFD sync data to identify KMP categories.